

Số: /STTTT-CNTT&BCVT
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và
nghiêm trọng trong các sản phẩm Microsoft
công bố tháng 02/2024

Tuyên Quang, ngày tháng 02 năm 2024

Kính gửi:

- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Ủy ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 210/CATTT–NCSC ngày 22/002/2024 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh khai thác lỗ hổng bảo mật cao và nghiêm trọng trong các sản phẩm Microsoft như sau:

I. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft

Ngày 13/02/2024, Microsoft đã phát hành danh sách bản vá tháng 02 với 72 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2024-21410** trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.
- 02 lỗ hổng an toàn thông tin **CVE-2024-21413, CVE-2024-21378** trong Microsoft Outlook cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-21399** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-21412** trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.
- Lỗ hổng an toàn thông tin **CVE-2024-21379** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-21384** trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-20673** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21351** trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.

Thông tin chi tiết các lỗ hổng an toàn thông tin xem tại Phụ lục kèm theo.

II. Các giải pháp phòng tránh

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại Phụ lục kèm theo).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại: 02432091616, thư điện tử: ncsc@ais.gov.vn

Trân trọng./.

Nơi nhận:

- Như trên;
- Ban Giám đốc sở (báo cáo);
- Các đơn vị thuộc Sở;
- Lưu: VT, CNTT&BCVT

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Văn Hiến

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN
TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /STTTT-CNTT&BCVT ngày / 02 /2024
của Sở Thông tin và truyền thông)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-21410	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
2	CVE-2024-21413 CVE-2024-21378	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise, Microsoft Outlook. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21378
3	CVE-2024-21399	<ul style="list-style-type: none"> - Điểm: CVSS: 8.3 (Trung bình) - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21399

		- Ảnh hưởng: Microsoft Edge (Chromium-based).	
4	CVE-2024-21412	<ul style="list-style-type: none"> - Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
5	CVE-2024-21379	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379
6	CVE-2024-21384	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft 365 Apps for Enterprise. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21384

7	CVE-2024-20673	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft Office, Skype for Business. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20673
8	CVE-2024-21351	<ul style="list-style-type: none"> - Điểm: CVSS: 7.6 (Cao) - Mô tả: Lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của Phụ lục.

3. Tài liệu tham khảo

<https://msrc.microsoft.com/update-guide/>

<https://www.zerodayinitiative.com/blog/2024/2/13/the-february-2024-security-update-review>